JOURNAL OF ALGEBRA 42, 121–135 (1976)

The Power Structure of p-Groups. I

AVINOAM MANN

Department of Mathematics, Hebrew University, Jerusalem, Israel

Communicated by B. Huppert

Received April 1, 1975

In this paper all groups are finite p-groups. For such a group, G, two characteristic subgroups are defined by

$$\Omega_n(G) = \langle a \in G \mid a^{p^n} = 1 \rangle,$$
$$\mho_n(G) = \langle a \in G \mid a = b^{p^n} \rangle \qquad \text{for some} \quad b \in G.$$

In this paper we are interested in the following statements:

(1) Each element of $\mho_n(G)$ is a p^nth power.

(2) Each element of $\Omega_n(G)$ has order p^n (at most)

(3) $|\mho_n(G)| = |G : \Omega_n(G)|$.

Generally, a p-group need not satisfy either of these three statements. It is well known that regular p-groups, as introduced by P. Hall ([2]; or see [3, III.10]) do satisfy all three statements. There exist, however, also non-regular p-groups satisfying them.

In this paper we call a p-group G a *P_i-group* ($i = 1, 2$ or 3) if G, as well as *all sections of* G, satisfy the statement (i), and a *P-group*, if G and its sections satisfy all three statements.

These properties P_1, P_2, P_3 are not independent. We shall see that $P_3 \Rightarrow P_2 \Rightarrow P_1$ (and thus $P = P_3$). This is established in Section 1 by investigating so-called minimal non-P_i-groups. Various criteria for a group to lie in one of the classes P_i are given in that section. Thus, possession of the property P_i depends only on sections of exponent p^2. Assuming Kostrikin's solution of the restricted Burnside problem for exponent p, we can restrict ourselves also to sections of a bounded class and order.

It turns out that P_2-groups can be characterized by the *inequalities* $|\mho_n(G)| \leqslant |G : \Omega_n(G)|$. Other results are: if all subgroups of $\Phi(G)$ have "few" generators, then G is P_1-group; G is a P_i-group if it has "many" factor groups which are P_i-groups.

In Section 2 we consider properties of P_i-groups similar to properties of regular groups. Both P_2 and P-groups are characterized in terms very similar to Hall's definition of regularity. We get commutation relations. Thus $[\mho_m(G), \mho_n(G)] \subseteq \mho_{m+n}(G)$ holds in P_1-groups, and $[\Omega_n(G), \mho_n(G)] = 1$ holds in P_2-groups. Also, P-groups possess bases. The theme in these results seems to be, that in theorems holding for regular groups, one has to replace elements by the subgroups they generate, to get theorems holding for P-groups.

In section 3 we show that the classes of P_i-groups are closed under direct products with groups of exponent p. On the other hand, if $G \times C$ is a P_i-group for all cyclic groups C, then G is regular.

In Section 4, we first consider 2-groups. It turns out, for instance, that a 2-group is a P_2-group if and only if it is modular. We conclude with some examples.

The notation and terminology are mostly standard. We use notation such as $Z(G \bmod K)$, when $K \triangle G$, for the subgroup H satisfying $H/K = Z(G/K)$. A *section* of G is a group H/K, where $K \triangle H \subseteq G$.

We conclude the introduction by mentioning some problems we consider worthy of a further study.

1. Investigate P_i-groups for $p = 3$.
2. Investigate metabelian P_i-groups.
3. Investigate the class of p-groups G having a normal series

$$\{1\} = G_e \triangle G_{e-1} \triangle \cdots \triangle G_0 = G$$

where $\exp G = p^e$ and each factor group G_i/G_{i+1} has exponent p.

4. Given m, study the class of groups in which products of elements of order p^n have orders p^{n+m} (at most), or in which products of p^{n+m}th powers are p^nth powers (this class contains, trivially, all groups of exponent p^{m+1}; it also contains all groups of class $(m+1)(p-1)$ or less, by Theorem 1 of [7]).

1

THEOREM 1. *If each section of exponent p^2 of G is a P_i-group* $(i = 1, 2)$ *or a P-group, so is G.*

Proof. a. $i = 1$. We may assume $\exp G > p^2$, hence $\exp \mho_1(G) > p$. Choose z of order p in $\mho_1(\mho_1(G)) \cap Z(G)$. By induction, $z = u^p$ for some $u \in \mho_1(G)$. Also by induction, given $a, b \in G$, we have $a^p b^p = c^p z^i = c^p(u^i)^p$ for some c and i. As $u \in \Phi(G)$, we have $G \neq \langle c, u\rangle$, so again by induction $c^p(u^i)^p = d^p$ for some $d \in \langle c, u\rangle$. Thus $\mho_1(G)$ consists only of p'th powers. Induction in $\mho_1(G)$ yields that $\mho_n(G)$ consists only of p^n'th powers, for $n > 1$.

b. $i = 2$. Let $a, b \in G$ have order p, and let Z be a minimal normal subgroup of G. Let $H = \langle a, b, Z\rangle$, then by induction H/Z hs exponent p, hence H has exponent p^2, so by assumption ab has order p. Thus all elements of $\Omega_1(G)$ have order p. This implies $\Omega_n(G) = \Omega_{n-1}(G \bmod \Omega_1(G))$, for $n > 1$, and by induction all elements of $\Omega_n(G)$ have order p^n at most.

c. Each section of exponent p^2 of G is a P-group. Let $N = \Omega_1(G) \cap \mho_n(G)$. Assume $N \neq 1$. By cases a and b, $\exp N = p$ and each element of N is a p^n'th power. It follows that $\Omega_n(G \bmod N) = \Omega_{n+1}(G)$ and $N = \mho_n(\Omega_{n+1}(G))$, so, by induction,

$$\begin{aligned} |G : \mho_n(G)| &= |G/N : \mho_n(G/N)| = |\Omega_n(G/N)| \\ &= |\Omega_{n+1}(G) : N| = |\Omega_n(\Omega_{n+1}(G))| = |\Omega_n(G)|. \end{aligned}$$

If $N = 1$, then $\mho_n(G) = 1$, hence $G = \Omega_n(G)$.

Theorem 1 also holds for the property P_3, since we shall prove below that P_3 is equivalent to P.

If Q is any group theoretical property, we term a group G a *minimal non-Q group*, if G does not enjoy the property Q, but all of its proper sections do.

PROPOSITION 2. *If a P_1-group G contains a subgroup E of exponent p^n and index p^k, then $|\mho_n(G)| \leqslant p^k$.*

Proof. First, let $k = 1$. Let Z be a minimal normal subgroup of G. By induction, $|\mho_n(G/Z)| \leqslant p$, hence $|\mho_n(G)| \leqslant p^2$. Assume $|\mho_n(G)| = p^2$. Then $\mho_n(G) \subseteq E$, and there exists a normal subgroup A such that $\mho_n(G) \subseteq \Phi(G) \subseteq A \subseteq E$ and $|G : A| = p^2$. If $a \in G$, then $a^p \in A$, hence $M = \langle a, A\rangle$ is a maximal subgroup of G (or $M = A$), $\langle a^{p^n}\rangle \in \mho_n(M)$, and $|\mho_n(M)| \leqslant p$ by induction. If $M_1, \dots, M_{p+1}$ are all the maximal subgroups containing A, we see that all p^n'th powers in G are contained in the union of the subgroups $\mho_n(M_i)$, each having order 1 or p, and at least one of which, $\mho_n(E)$, is trivial. But then of the $p + 1$ subgroups of order p of $\mho_n(G)$ there exists one which does not consist of p^n'th powers, contrary to G being a P_1-group.

Now let $k > 1$. Let M be a maximal subgroup of G containing E. Then $|\mho_n(M)| \leqslant p^{k-1}$, by induction. By the previous case in $G/\mho_n(M))$ we have $|\mho_n(G) : \mho_n(M)| \leqslant p$, so $|\mho_n(G)| \leqslant p^k$.

In the following, we use sometimes Kostrikin's solution of the restricted Burnside problem [4], according to which a 2-generator finite group of exponent p has a bounded order. We are going to star all statements relying on Kostrikin's result. Assuming this result, we denote by $c(p)$ and $p^{n(p)}$, respectively, the maximum class and order of a 2-generator finite group of exponent p.

THEOREM 3. *Let G be a minimal non-P_1 group. Then*

a. *G can be generated by two elements and has exponent p^2.*

b. *$\Phi(G) = Z_{c-1}(G)$ has exponent p. (Here $c = \operatorname{cl} G$).*

c. *$Z(G) = \mho_1(G)$ is elementary abelian of order p^2.*

d. *Each proper subgroup of G has smaller class than G.*

e*. $\operatorname{cl} G \leqslant c(p) + 1$, $|G| \leqslant p^{n(p)+2}$.

Proof. Since G is not a P_1-group, there exist two elements, a, b, say, such that $a^p b^p$ is not a p'th power. By minimality $G = \langle a, b\rangle$. By Theorem 1, $\exp G = p^2$.

Assume $\exp \Phi(G) = p^2$, then one can find a minimal normal subgroup $Z \subseteq \mho_1(\Phi(G))$. Since G/Z is a P_1-group, we get $a^p b^p = c^p z$, for some $c \in G$, $z \in Z$. Since $\Phi(G)$ is a P_1-group, we have $z = u^p$, $u \in \Phi(G)$. Now $\langle c, u\rangle \neq G$, so $a^p b^p = c^p u^p$ is a p'th power in $\langle c, u\rangle$, a contradiction.

Now $Z(G) \subseteq \Phi(G)$, otherwise we can find a pair of generators for G, one of which is central, and G is abelian. Thus $Z(G)$ is elementary abelian. If $Z \subseteq Z(G)$ has order p, then as above we obtain $a^p b^p = c^p z$, where $1 \neq z \in Z$. Thus $z = a^p b^p c^{-p} \in \mho_1(G)$, so $Z \subseteq \mho_1(G)$ and $Z(G) \subseteq \mho_1(G)$.

Any element $x \in G$ is contained in some maximal subgroup M of G. By Proposition 2, $|(\mho_1 M)| \leqslant p$, and $\mho_1(M) \vartriangle G$, so $\mho_1(M) \subseteq Z(G)$. As $x^p \in \mho_1(M)$, we have $\mho_1(G) \subseteq Z(G)$. Moreover, choosing M such that $|\mho_1(M)| = p$, and applying Proposition 2 to $G/\mho_1(M)$, we get $|\mho_1(G)| \leqslant p^2$. Equality obtains, as any group with $|\mho_1(G)| = p$ is a P_1-group.

It follows that $G/Z(G)$ is a 2-generator group of exponent p, hence e holds. For d and $\Phi(G) = Z_{c-1}(G)$ see [6, Prop. 12].

COROLLARY 4. *A P_2-group is a P_1-group.*

Proof. By induction we may assume that G is a minimal non-P_1-group. Since G is not P_1, of the $p + 1$ subgroups of order p of $Z(G)$ at least one does not consist of p'th powers. Since $|\mho_1(M)| \leqslant p$ for each maximal subgroup M of G, we can find two maximal subgroups, M and M_1, such that $\mho_1(M) = \mho_1(M_1) = Z$ (say; or $\mho_1(M_1) = 1$). Then G/Z, being a P_2-group, is of exponent p, so $\mho_1(G) = Z$, a contradiction.

Indeed, it follows from the proof, that it suffices to require that each proper section of G is a P_2-group.

COROLLARY 5. *If each subgroup of $\Phi(G)$ can be generated by $\frac{1}{2}(p + 1)$ elements, then G is a P_1-group (here p is odd).*

Proof. It suffices to assume that G is a minimal non-P_1-group, and show that then $\Phi(G)$ contains an elementary abelian subgroup of order $\geqslant \frac{1}{2}(p + 3)$.

If $clG = c$, then $c \geqslant p$, and Theorem 3 implies that $Z(G)G_{\frac{1}{2}(c+1)}$ is such a subgroup.

THEOREM 6. *Let G be a minimal non-P_2-group. Then*

a. *G can be generated by two elements of order p*; $\exp G = p^2$.

b. *G contains a maximal subgroup of exponent p. In particular*, $\exp \Phi(G) = p$; *moreover*, $\Phi(G) = G' = Z_{c-1}(G)$.

c. *$Z(G) = \mho_1(G)$ has order p.*

d. *G is a minimal non-P group, and a P_1-group.*

e. *Each proper section of G has smaller class than G.*

f*. $clG \leqslant c(p) + 1$, $|G| \leqslant p^{n(p)+1}$.

Proof. By Theorem 1, $\exp G = p^2$. As G does not satisfy P_2, there exist two elements $a, b \in G$ such that $a^p = b^p = 1$ but $(ab)^p \neq 1$. By minimality, $G = \langle a, b \rangle$. Let $M = \langle a^G \rangle$, then M is a proper subgroup of G, and is generated by conjugates of a, so $\exp M = p$. Since $G = M\langle b \rangle$ and $b^p = 1$, we have $|G : M| = p$. Since $\Phi(G) \subseteq M$, also $\exp \Phi(G) = p$.

Let Z be a minimal normal subgroup of G, then $G/Z = \langle aZ, bZ \rangle$, so $\exp G/Z = p$ and $Z = \mho_1(G)$. Thus Z is unique. Also, $Z = Z(G)$ since $Z(G) \subseteq \Phi(G)$ is elementary abelian. Also, $Z \subseteq G'$, so $\Phi(G) = G'$.

Proposition 12 of [6] implies that $\Phi(G) = Z_{c-1}(G)$ and that subgroups of G have smaller class than G, while proper quotients of G are all quotients of G/Z and so have smaller class than G.

Let H be a proper section of G. To prove the first part of (d) we have only to show that $|H : \Omega_1(H)| = |\mho_1(H)|$. If $\exp H = p$, both numbers are 1, while if $\exp H = p^2$, both numbers are p, by (b) and (c). The second part of (d) follows from $|\mho_1(G)| = p$. Finally, (f*) follows as in Theorem 3.

THEOREM 7. *The group G is a P_2-group if and only if all sections H of G satisfy* $|\mho_n(H)| \leqslant |H : \Omega_n(H)|$.

Proof. If G is a P_2-group, the result follows by combining Proposition 2 with Corollary 4. Conversely, if G is not a P_2-group, some section H of G is a minimal non-P_2 group, which, by Theorem 6(a) and (c), satisfies $|\mho_1(H)| = p$, $|H : \Omega_1(H)| = 1$.

COROLLARY 8. *A P_3-group is a P-group.*

A group constructed by Blackburn [3; III.10.15], for which $|G| = p^{p+1}$, $|\Omega_1(G)| = p^{p-1}$ and $|\mho_1(G)| = p$ shows that P_2-groups are not always P_3-groups. This group is also an example of minimal non-P group which is a P_2-group.

THEOREM 9. *Let G be a minimal non-P-group. Then*

a. *G has two generators and exponent p^2.*

b. *Either $\Omega_1(G) = G$ or $\Omega_1(G) = \Phi(G)$. In any case, $\Phi(G) = G' = Z_{c-1}(G)$ and this subgroup has exponent p.*

c. *$Z(G) = \mho_1(G)$ has order p.*

d. *Each proper section of G has smaller class than G.*

e*. $\mathrm{cl}\, G \leqslant c(p) + 1$, $| G | \leqslant p^{n(p)+1}$.

Proof. If G is not a P_2-group, everything follows from Theorem 6. Assume then, that G is a P_2-group. Then the only way in which G can fail to be a P-group is by satisfying the inequality

$$| G : \Omega_1(G)| \neq | \mho_1(G)|. \tag{4}$$

Let $Z \subseteq \mho_1(G)$ be a minimal normal subgroup of G. Then

$$| G : \mho_1(G)| = | G/Z : \mho_1(G/Z)| = | \Omega_1(G/Z)|.$$

Denote $H = \Omega_1(G \bmod Z)$. Then $Z = \mho_1(H)$. If $H \neq G$, then

$$| \Omega_1(G/Z)| = | H : Z | = | H : \mho_1(H)| = | \Omega_1(H)| = | \Omega_1(G)|$$

contradicting (4). Thus $G = H$, i.e. $Z = \mho_1(G)$. It follows that Z is unique.

Let M be a maximal subgroup of G, then $| \mho_1(M)| \leqslant p$, so that $| M : \Omega_1(M)| \leqslant p$ and $| G : \Omega_1(G)| \leqslant p^2$. Since G is a P_2-group, we have $G \neq \Omega_1(G)$, and by (4) we must have $| G : \Omega_1(G)| = p^2$. Now for *any* maximal subgroup M we get $\Omega_1(G) = \Omega_1(M)$, hence $\Omega_1(G) = \Phi(G)$. Since $Z(G) \subseteq \Phi(G)$, we find now that $Z(G)$ is elementary abelian and so $Z(G) = Z$. The rest follows as before.

Remark. In [5] we investigated minimal nonregular groups, and proved in particular that for those groups, we have $\mathrm{cl}\, G \leqslant c(p) + 1$. This result was then improved by Groves [1], using variety methods, to $\mathrm{cl}\, G \leqslant c(p)$, for $p > 3$, which is best possible. We do not know if a similar improvement is possible for the minimal groups of this paper. Examples for which $\mathrm{cl}\, G = c(p)$ will be constructed in Section 4.

The following is obvious.

COROLLARY 10*. *A group G has the property P (or P_2, or P_1) if and only if all sections of G of exponent p^2, class at most $c(p) + 1$ and order at most $p^{n(p)+1}$ ($p^{(n(p)+2}$ for P_1) possess the same property.*

COROLLARY 11. *Let the group G contain an elementary abelian central* *subgroup N of order p^2, such that G/K is a P-group (P_2-group) for all $1 \neq K \subseteq N$. Then G is a P-group (P_2-group).*

For the proof, see the proof of [6, Prop. 2]. Similarly one obtains

COROLLARY 12. *Let the group G contain an elementary abelian central subgroup N of order p^3, such that G/K is a P_1-group for all $1 \neq K \subseteq N$. Then G is a P_1-group.*

2

Our first aim here is the following result.

THEOREM 13. *If E is a normal subgroup of exponent p^n of a P_1-group G, then $[\mho_n(G), E] = 1$.*

From this follows immediately

COROLLARY 14. *In a P_1-group, $[\mho_m(G), \mho_n(G)] \subseteq \mho_{n+m}(G)$.*

COROLLARY 15. *In a P_2-group, $[\mho_n(G), \Omega_n(G)] = 1$.*

To prove Theorem 13 we take any element $a \in G$ and try to prove $[a^{p^n}, E] = 1$. It is enough to consider the group $\langle a, E\rangle$, and for this group the theorem follows from the following result.

PROPOSITION 16. *Let the P_1-group G contain a normal subgroup E of exponent p^n such that G/E is cyclic of order p^k. Then $\mho_n(G)$ is a cyclic central subgroup of G of order at most p^k.*

Proof. For $k = 1$ everything follows from Proposition 2. Hence we assume from now on that $k > 1$. We may also assume that E is maximal among the normal subgroups of G having exponent p^n and cyclic factor group. Under these assumptions we shall prove the following stronger statement: *$\mho_n(G)$ is central cyclic of order exactly p^k, and if $G = \langle a, E\rangle$, then $\mho_n(G) = \langle a^{p^n}\rangle$* (this statement does not hold for $k = 1$. For example, in $C_p \int C_p$ we may have $G = \langle a, E\rangle$ with $a^p = 1$).

First, assume $n = 1$. Let $E \subseteq F \triangle G$ with $|F : E| = p$. Since E is maximal, $Z = \mho_1(F) \neq 1$, and by the case $k = 1$, $|Z| = p$. We employ induction in G/Z, in which group F/Z has exponent p. Thus $\mho_1(G)/Z = \mho_1(G/Z)$ is cyclic, of order p^{l-1}, say. Then $\mho_1(G)$ is, in any case, abelian, and if noncyclic, it can be written as $A \times B$, where $|A| = p$, $|B| = p^{l-1}$.

If $l > 2$, then $\Omega_1(B) \triangle G$, and $\mho_1(G)/\Omega_1(B)$ is not cyclic, contrary to the inductive assumption. Let $l = 2$. Then $\mho_1(G)$ is elementary abelian, and $\exp G = p^2$. Since $k > 1$, we have $\mho_1(G) \not\subseteq E$, but $Z \subseteq \mho_1(G)$ and $Z \subseteq E$

(by maximality of E). Let $G = \langle a, E\rangle$. Then $a^p \notin E$, by $k > 1$, and so $\mho_1(G) = \langle a^p, Z\rangle$. If $x \in E$, we obtain in the same way that $\mho_1(G) = \langle (ax)^p, Z\rangle$. Since $Z \subseteq Z(G)$, we find that $\mho_1(G)$, so also a^p, centralize ax. Thus a^p commutes with x, and so with E, so $a^p \in Z(G)$. But then $\langle a^p, E\rangle$ has exponent p and properly contains E, a contradiction. Therefore, $\mho_1(G)$ is cyclic of order p^l.

Now maximality of E implies $|\mho_1(G) \cap E| = p$. Therefore $|\mho_1(G)E| = p^{l-1}|E|$, also $|G : \mho_1(G)E| = p$ so $|G| = p^l|E|$, i.e. $l = k$.

Finally, let $G = \langle a, E\rangle$. Then $a^{p^{k-1}} \notin E$, so $a^{p^{k-1}}$ does not lie in the unique subgroup of order p of $\mho_1(G)$, so $a^{p^k} \neq 1$, a has order exactly p^{k+1}, and $\mho_1(G) = \langle a^p\rangle$. For any $x \in E$, we find also that $\mho_1(G) = \langle (ax)^p\rangle$, and therefore a^p commutes with ax and $a^p \in Z(G)$ as before. This concludes the proof for $n = 1$.

For $n > 1$, let $N = \mho_1(E)$. Then in G/N we have E/N as a normal subgroup of exponent p and cyclic factor group of order p^k, and E/N is maximal relative to these properties. By the case $n = 1$ we find that $\mho_1(G)/N$ is cyclic of order p^k, and if $G = \langle a, E\rangle$, then $\mho_1(G)/N = \langle a^pN\rangle$. In $\mho_1(G)$ there are two subgroups K and L, defined uniquely by $N \subseteq K \subseteq L \subseteq \mho_1(G)$, $|L : K| = |K : N| = p$.

If N is not maximal among the subgroups of $\mho_1(G)$ of exponent p^{n-1}, then $\exp K = p^{n-1}$. Moreover, in G/K both EK/K and L/K have exponent p and L/K is central, so EL/K has exponent p and $\exp EL = p^n$. By maximality of E we get $L \subseteq E$ and, therefore $|L : N| = p$, which is not true. Thus $\mho_1(G)$ and N satisfy our assumptions with exponent p^{n-1}. By induction we get that $\mho_n(G) = \mho_{n-1}(\mho_1(G))$ is cyclic of order p^k, and if $G = \langle a, E\rangle$ then, because $\mho_1(G) = \langle a^p, N\rangle$, also $\mho_n(G) = \langle a^{p^n}\rangle$. For $x \in E$, we get also $\mho_n(G) = (ax)^{p^n}$ which implies as before that $\mho_n(G) \subseteq Z(G)$.

Passing now to P_2-groups, we first give an alternative proof of Corollary 15. Let G be a P_2-group, and let $a, b \in G$, $b^{p^n} = 1$. In proving $[a^{p^n}, b] = 1$, we may assume $G = \langle a, b\rangle$. Let z be a central element of order p, and denote $Z = \langle z\rangle$, $N = \langle z, a^{p^n}\rangle$. Since, by induction, $a^{p^n} \in Z(G \bmod Z)$, we have $N \triangle G$. In G/N, both aN and bN have order p^n, so $\exp G/N \leqslant p^n$, and in particular $(ab)^{p^n} \in N$. Considering ab instead of a, we get in the same way $a^{p^n} \in \langle Z, (ab)^{p^n}\rangle$, so $N = \langle Z, (ab)^{p^n}\rangle$. It follows that ab, as well as a, centralizes N, so also $b \in C_G(N)$ and so b centralizes a^{p^n}.

Corollary 17. *If G is a P_2-group, $a, b \in G$ and $b^{p^n} = 1$, then $\langle a^{p^n}\rangle = \langle (ab)^{p^n}\rangle$.*

Proof. Assuming $G = \langle a, b\rangle$, Corollary 15 implies that $\langle a^{p^n}\rangle \triangle G$, hence $(ab)^{p^n} \in \langle a^{p^n}\rangle$, and similarly $a^{p^n} \in \langle (ab)\rangle^{p^n}\rangle$.

THEOREM 18. *The group G is a P_2-group if and only if it satisfies: given $a, b \in G$, there exist integers i, j such that*

$$\text{(A)} \qquad (ab)^p = a^{ip}b^{jp}u_1{}^p \cdots u_l{}^p, \qquad u_k \in \langle a, b\rangle'$$

Proof. Let G be a P_2-group. We may assume that $G = \langle a, b\rangle$, and also that $\exp G' = p$. Then $b^{-1}\langle a^p\rangle b = (b^{-1}ab)^p = \langle (a[a, b])^p\rangle = \langle a^p\rangle$ by Corollary 17, so $\langle a^p\rangle \triangle G$. Similarly, $\langle b^p\rangle \triangle G$. If $N = \langle a^p, b^p\rangle$, then G/N has exponent p, so $(ab)^p \in N$, which implies (A).

Conversely, let G satisfy (A). Let $a, b \in G$ have order p. Since $\langle a^G\rangle \neq G$, and $\langle a^G\rangle$ is generated by conjugates of a, of order p, we get by induction that $\exp\langle a^G\rangle = p$. We may assume $G = \langle a, b\rangle$. Then $G/\langle a^G\rangle$ is cyclic, so $G' \subseteq \langle a^G\rangle$, and $\exp G' = p$. Now (A) yields that ab has order p. We have thus proved that $\exp \Omega_1(G) = p$, and we can apply induction on n to $G/\Omega_1(G)$ to conclude that $\exp \Omega_n(G) = p^n$. As condition (A) is inherited by sections of G, G is a P_2-group.

For P-groups, we first sharpen Corollary 17.

PROPOSITION 19. *Let G be a P-group, and let $a, b \in G$. Then $\langle a^{p^n}\rangle = \langle b^{p^n}\rangle$ if and only if there exist integers i, j, $ij \not\equiv 0(p)$, such that $(a^ib^j)^{p^n} = 1$.*

Proof. If i, j exist then, by Corollary 17

$$\langle a^{p^n}\rangle = \langle (a^{-i})^{p^n}\rangle = \langle (a^{-i}\cdot a^ib^j)^{p^n}\rangle = \langle (b^j)^{p^n}\rangle = \langle b^{p^n}\rangle.$$

Let $\langle a^{p^n}\rangle = \langle b^{p^n}\rangle = N$. We again assume $G = \langle a, b\rangle$. If $N = 1$, everything is trivial. Let $N \neq 1$, then $\exp G/N = p^n$, so $N = \mho_n(G)$, and if $|a| = p^{n+k}$, then $|G : \Omega_n(G)| = |\mho_n(G)| = p^k$. However, a has order p^k $(\bmod\, \Omega_n(G))$, so $G = \langle a, \Omega_n(G)\rangle$ and in particular $b \equiv a^i$ $(\bmod\, \Omega_n(G))$, where $i \not\equiv 0(p)$ since $|a| = |b|$, i.e., $(a^{-i}b)^{p^n} = 1$.

THEOREM 20. *A p-group G of exponent p^2 is a P-group if and only if for each pair $a, b \in G$ there exists a permutation π of $\{1, 2,..., p-1\}$ such that for each $j = 1,..., p-1$ there exists an i satisfying*

$$\text{(B)} \qquad (ab^j)^p = a^{ip}b^{i\pi(j)p}u_1{}^p \cdots u_l{}^p, \qquad u_k \in \langle a, b\rangle'.$$

Proof. Let G be a P-group. We may assume that $G = \langle a, b\rangle$ and that $\exp G' = p$. Then Corollary 17 yields

$$b^{-1}\langle a^p\rangle b = \langle (b^{-1}ab)^p\rangle = \langle a[a, b]\rangle^p = \langle a^p\rangle,$$

so $\langle a^p\rangle \triangle G$ (hence $a^p \in Z(G)$), and similarly $\langle b^p\rangle \triangle G$. Then $G/\langle a^p, b^p\rangle$, generated by elements of order p, is of exponent p, so that $\mho_1(G) = \langle a^p, b^p\rangle$.

Now if $a^p = 1$ or $b^p = 1$, we can pick π arbitrarily. Assume $\langle a^p \rangle = \langle b^p \rangle \neq 1$, then $|\mho_1(G)| = p$ implies $|G : \Omega_1(G)| = p$. Since $\Phi(G) \subseteq \Omega_1(G)$ and $G = \langle a, b \rangle$, there exists a unique $j \in \{1,\dots, p-1\}$ such that $\Omega_1(G) = \langle \Phi(G), ab^j \rangle$. Let k be such that $b^p = a^{kp}$, then we can choose as π any permutation satisfying $k\pi(j) \equiv p - 1(p)$.

Finally, let $\langle a^p \rangle \neq \langle b^p \rangle$, so $|\mho_1(G)| = p^2$. Then $|G : \Omega_1(G)| = p^2$, so $\Omega_1(G) = \Phi(G)$. The maximal subgroups of G are generated by $\Phi(G)$ and one of the elements b, a, ab^j, $j = 1,\dots, p-1$. The map $M \to \mho_1(M)$ maps maximal subgroups to subgroups of order p of $\mho_1(G)$. As this map is onto, it is 1–1. To the maximal subgroups corresponding to a and b there correspond $\langle a^p \rangle$ and $\langle b^p \rangle$, so to the maximal subgroup corresponding to ab^j there corresponds a subgroup $\langle a^p b^{kp} \rangle$ for some $k = 1,\dots, p-1$, and here $j \to k$ is a permutation, which can be taken as π because $(ab^j)^p = (a^p b^{kp})^i$, some i.

Conversely, assume that G satisfies (B). By Theorem 18, G is a P_2-group, and we may assume that it is a minimal non-P-group. By Theorem 9, $G = \langle a, b \rangle$ and $\Omega_1(G) = \Phi(G)$, so $\langle a^p \rangle = \langle b^p \rangle = \mho_1(G)$, and we may assume that $a^p = b^p$. Applying (B), we choose j so that $\pi(j) = p - 1$, and then (B) implies that $(ab^j)^p = 1$, contrary to $\Omega_1(G) = \Phi(G)$.

Proposition 21. *If G is a P-group, then $\mho_n(G') \subseteq [\mho_n(G), G]$.*

Proof. We may assume that $[\mho_n(G), G] = 1$. Then, for any $a, b \in G$, $(a^{-1}ba)^{p^n} = a^{-1}b^{p^n}a = b^{p^n}$ so, by Proposition 19, there exist i and j such that $(b^i a^{-1} b^j a)^{p^n} = 1$ and, since $j \not\equiv 0(p)$, $a^{-1}ba \in \langle b, \Omega_n(G) \rangle$. It follows that each cyclic subgroup, therefore each subgroup, of $G/\Omega_n(G)$ is normal. As the quaternion group is not a P-group, it follows that $G/\Omega_n(G)$ is abelian, i.e., $G' \subseteq \Omega_n(G)$ and $\mho_n(G') = 1$.

For any P_1-group, G, define $\omega_n = \omega_n(G)$ for $n = 1, 2,\dots, e$, where $\exp G = p^e$, by:

$$p^{\omega_n} = |\mho_{n-1}(G) : \mho_n(G)|.$$

As in [2], define μ_m to be the number of the ω_n's which are $\geqslant m$. Then $\mu_1 = e$.

Proposition 22. *Let G be a P_1-group, $H \subseteq G$ and $K \triangle G$. Then*

$$\omega_n \geqslant \omega_{n+1}, \qquad \mu_n \geqslant \mu_{n+1}$$

$$\omega_n(H) \leqslant \omega_n(G),\ \mu_n(H) \leqslant \mu_n(G),\ \omega_n(G/K) \leqslant \omega_n(G),\ \mu_n(G/K) \leqslant \mu_n(G).$$

Proof. In $\mho_{n-1}(G)/\mho_{n+1}(G)$, Proposition 2 implies that

$$|\mho_n(G)/\mho_{n+1}(G)| = |\mho_1(\mho_{n-1}(G)/\mho_{n+1}(G))| \leqslant |\mho_{n-1}(G)/\mho_n(G)|,$$

which is the first inequality, and the second one is trivial. As in [2], it is enough to prove the inequalities involving ω_n in the second line. The one for G/K is trivial. Since $\omega_n(G) = \omega_1(\mho_{n-1}(G))$, it is enough to prove $\omega_1(H) \leqslant \omega_1(G)$. Now if $K \triangle G$, then working in $G/\mho_1(K)$ we find, by Proposition 2,

$$|K : \mho_1(K)| \leqslant |G/\mho_1(K) : \mho_1(G)/\mho_1(K)| = |G : \mho_1(G)|,$$

so $\omega_1(K) \leqslant \omega_1(G)$. Since H is subnormal in G, we get $\omega_1(H) \leqslant \omega_1(G)$ by successive applications of the normal case.

A set of elements $a_1, \dots, a_r$ ($\neq 1$) of a p-group G, of orders $e_1, \dots, e_r$ respectively, is termed a *basis* for P, if each element a of G can be written uniquely as

$$a = a_1^{n_1} \cdots a_r^{n_r}, \qquad 0 \leqslant n_i < e_i .$$

THEOREM 23. *A P-group G possesses a basis. Moreover, for any such basis $r = \omega_1(G)$ and the orders $e_1, \dots, e_r$ are the numbers $p^{\mu_1}, \dots, p^{\mu_r}$.*

The proof is identical to P. Hall's proof of this theorem for regular groups [2, (4.5)] (at one point we have to use Proposition 19 instead of the corresponding result for regular groups).

Other p-groups may have bases. For example, let G be a group containing a regular maximal subgroup G_1 such that all elements outside G_1 have order p. Then adjoining any element outside G_1 to a basis of G_1 we get a basis for G_1. Moreover, any section of G is either regular, or enjoys the same properties we required for G. By results of Blackburn, if H is a p-group of maximal class, then we can take $G = H/Z(H)$ [3, III.14.13(b)].

Groups G of the type discussed in the previous paragraph are P_1-groups, because $\mho_1(G) = \mho_1(G_1)$, and usually not P_2-groups, because $G = \Omega_1(G)$. Indeed, we have: *if all sections of a P_2-group G have a basis, then G is a P-group.* Thus, the argument of [2, 4.51] shows that $|\mho_n(G)| \geqslant |G : \Omega_n(G)|$ which, together with Theorem 7, yields our claim.

3

We now pass to direct products.

THEOREM 24. *Let G be a P_i-group ($i = 1$, 2 or 3) and H a group of exponent p. Then $G \times H$ is a P_i-group.*

Proof. Let $K \subseteq G \times H$ and $N \triangle K$. We want to show that K/N is a P_i-group. We may assume that K projects on the whole of G. Let $a = (x, \alpha)$ and $b = (y, \beta)$ be in K.

If G is a P_1-group, write $x^{p^n}y^{p^n} = z^{p^n}$, for some $z \in G$, and find a $\gamma \in H$ such that $(z, \gamma) \in K$, then

$$a^{p^n}b^{p^n} = (x^{p^n}y^{p^n}, \alpha^{p^n}\beta^{p^n}) = (z^{p^n}, 1) = (z, \gamma)^{p^n}$$

which shows that K (and K/N) are P_1-groups.

For P_2, assume that $(aN)^{p^n} = (bN)^{p^n} = 1$, i.e., $a^{p^n} \in N$ and $b^{p^n} \in N$. Then $a^{p^n} = (x^{p^n}, 1) \in N \cap G$ and also $(y^{p^n}, 1) \in N \cap G$. Since K projects on G, we have $N \cap G \triangle G$, so by considering $G/N \cap G$ we obtain

$$(ab)^{p^n} = ((xy)^{p^n}, 1) \in N \cap G, \qquad (aN \cdot bN)^{p^n} = 1.$$

Now let G be a P_3-group. Considering G, H, and K as subgroups of $G \times H$ we see that $\mho_n(K)$ is mapped onto $\mho_n(G)$ and that $\mho_n(K) \subseteq \mho_n(G \times H) = \mho_n(G)$, so $\mho_n(K) = \mho_n(G)$. Also $\Omega_n(K)$ is mapped onto $\Omega_n(G)$, with kernel $\Omega_n(K) \cap H = K \cap H$, so

$$| K : \Omega_n(K)| = | G : \Omega_n(G)| = | \mho_n(G)| = | \mho_n(K)|.$$

For K/N, let first $G \cap N \neq 1$, then K/N is a section of $G/G \cap N \times H$, and we use induction. If $N \cap G = 1$, then $N \cong NG/G$ has exponent p, so $N \subseteq \Omega_n(K)$. If $a \in K$ and $(aN)^{p^n} = 1$ in K/N, then $a^{p^n} \in N \cap G = 1$, so $a \in \Omega_n(K)$. Thus $\Omega_n(K)$ maps onto $\Omega_n(K/N)$, with kernel N. From $N \cap G = 1$ follows also $N \cap \mho_n(K) = 1$, so

$$\begin{aligned} | K/N : \Omega_n(K/N)| &= | K : \Omega_n(K)| = | \mho_n(K)| = | \mho_n(K)/\mho_n(K) \cap N | \\ &= | \mho_n(K)N/N | = | \mho_n(K/N)|. \end{aligned}$$

For groups of exponent larger than p, however, we have

THEOREM 25. *Let G be a group of exponent p^e and C a cyclic group of order p^e. If $G \times C$ is a P_1-group, then G is regular.*

This result implies both Proposition 1 and Theorem 7 of [6].

Proof. We may assume that G is a minimal irregular group, as described in [5]. In particular, from the calculation in the proof of Theorem 2(h) of [5] it follows that G can be generated by two elements, a and b, such that $(ab)^p \neq a^p b^p$ and a and b can be chosen to lie in any two prescribed maximal subgroups of G. We can always assume that a has order p^e. Let $C = \langle c \rangle$, and consider the subgroup $K = \langle (a, c), (b, 1) \rangle$ of $G \times C$. For any $u \in K$ we find

$$u = \Pi(a, c)^{\epsilon_k}(b, 1)^{\delta_k}, \qquad u = (a^i b^j d, c^i), \qquad d \in G', \qquad i = \Sigma\epsilon_k .$$

First, suppose that we can choose b of order p. For some $1 \neq t \in G'$ we have $(ab)^p = a^p b^p t$, so

$$((a, c)(b, 1))^p = (ab, c)^p = (a^p b^p t, c^p) = (a, c)^p (b, 1)^p (t, 1),$$

so $(t, 1) \in \mho_1(H)$. If $(t, 1) = u^p$, u as above, then

$$(t, 1) = ((a^i b^j d)^p, c^{ip}), \qquad c^{ip} = 1, \qquad p^{e-1} \mid i.$$

Thus $a^i \in Z(G)$ and

$$(a^i b^j d)^p = a^{ip}(b^j d)^p = 1, \qquad u^p = 1,$$

because $\langle b, d\rangle$ is regular and b and d have order p, a contradiction.

If b cannot be chosen of order p then, again by [5], $e = 2$ and a and b have order p^2. Then a^p and b^p are powers of each other, so

$$(a^p, c^p) \in \mho_1(H), (b^p, 1) \in \mho_1(H) \Rightarrow (1, c^p) \in \mho_1(H).$$

It is easy to see, however, that we cannot have $(1, c^p) = u^p$ in this case, for u as above.

In the next section we shall construct, for $p > 2$, a nonregular P-group G of exponent p^2. It follows from the results of this section that we have: $G \times H$ is a P_1-group if and only if H has exponent p.

4

For $p = 2$ the minimal groups described in Theorems 3, 6 and 9 are easy to determine. Let D, Q and R, S be, respectively, the dihedral group of order 8, the quaternion group, and the groups of order 16 defined by

$$R = \langle a, b \mid a^4 = b^4 = 1, b^{-1}ab = a^3\rangle,$$
$$S = \langle a, b \mid a^4 = b^4 = 1, b^{-1}ab = a^3 b^2\rangle$$

then R and S are the only minimal non-P_1-groups, D is the unique minimal non-P_2-group, and D and Q are the only minimal non-P-groups.

If G and H are groups, then G is termed *H-free* if no section of G is isomorphic to H. It is known that the D-free 2-groups are exactly the so-called modular 2-groups [8], and that a modular 2-group involves Q if and only if it is Hamiltonian. It also follows from [8] that a D-free and Q-free group of exponent 4 is abelian. Thus our remarks yield

THEOREM 26. *Let G be a 2-group. Then*

a. *G is a P_1-group if and only if it is R-free and S-free.*

b. *G is a P_2-group if and only if it is D-free, equivalently, if and only if it is modular.*

c. *The following are equivalent.*

(i) *G is a P-group.*

(ii) *G is both D-free and Q-free.*

(iii) *G is a nonhamiltonian modular group.*

(iv) *All sections of G of order* 8 *are abelian.*

(v) *All sections of G of exponent* 4 *are abelian.*

The last clause of this theorem raises the question, whether P-groups of exponent p^2 are always regular. We now show, that for each odd p there exists a nonregular P-group of exponent p^2.

Start with the direct product $H = \langle a_0 \rangle \times \langle a_1 \rangle \times \cdots \times \langle a_{p-2} \rangle$, where a_0 has order p^2 and the other a_i's have order p. Denote $a_{p-1} = a_0^{kp}$, where $k \not\equiv -1(p)$. Define an automorphism σ of H by $a_i^\sigma = a_i a_{i+1}$, $i = 0, 1, \ldots, p-2$. Then $a_{p-1}^\sigma = a_{p-1}$, and it is easy to verify that

$$a_0^{\sigma^i} = a_0 a_1{}^i \cdots a_n^{\binom{i}{n}} \ldots, \quad \sigma^p = 1.$$

Let G be the semidirect product $H\langle b \rangle$, where b induces σ on H and $b^p = 1$. Then G has order p^{p+1} and class p. All sections of G are regular, being of order p^p or less, but G itself, being of maximal class, is not. Now $Z = \langle a_{p-1} \rangle \triangle G$, and G/Z is generated by elements of order p, hence is of exponent p, so that $\mho_1(G) = Z$. To verify that G is a P-group, it is enough to show that $|\Omega_1(G)| = p^p$. Any element of G can be written as $x = b^i a_0{}^j c$, where $c \in G'$. If $i \not\equiv 0(p)$, let $il \equiv 1(p)$, then $x^l = b a_0{}^n d$, for some n and some $d \in G'$. x and x^l have the same order, and $(x^l)^p = (ba_0{}^n)^p$. By [3, III.9.5] we have

$$(ba_0{}^n)^p = b^p a_0^{np}[a_0{}^n, b, \ldots, b] = a_0^{np}[a_0, b, \ldots, b]^n = a_0^{n(k+1)p}$$

(the b in the commutators appears $p-1$ times), and this is 1 only if $p \mid n$. It follows that $\Omega_1(G) = \langle a_1, \ldots, a_{p-1}, b \rangle$ is indeed of order p^p.

The exceptional case $k \equiv -1$ above appears in an example of Blackburn [3, III.10.15]. (In that reference it is mistakingly stated that $k \equiv 1(p)$.) The group of that example, also of order p^{p+1} and class p, has $|\mho_1(G)| = p$, $\Omega_1(G)$ of order p^{p-1} and exponent p, and is thus a P_2-group and a minimal non-P-group. Also, the wreath product of two groups of order p is a minimal non-P_2-group. Thus there exist such groups of class p.

We now repeat a construction of [6]. Let G be a minimal irregular group, with $G = \langle a, b \rangle$, and let B be any group of exponent p and class $c > p$, also generated by two elements, $B = \langle x, y \rangle$. In $G \times B$ consider the subgroup $H = \langle (a, x), (b, y) \rangle$. Let Z be the minimal normal subgroup of G, then

$Z = \mho_1(H)$. Let K be any normal subgroup of H, maximal such that $K \cap Z = 1$. Then H projects onto G, $K \cap G \triangle H$, and $K \cap G$ is projected onto itself, so $K \cap G \triangle G$, hence $K \cap (H \cap G) = K \cap G = 1$. Thus H is a subdirect product of H/K and of $H/H \cap G$, of exponent p. By Theorem 24 H/K is a P_i-group if and only if H is, and H is a P_i-group if and only if G is. It is shown in [6], that H/K is minimal irregular, and can be taken to have class c. Taking G as one of the groups of orders p^{p+1} above, we see that we can arrange to have H/K of any class between p and $c(p)$, and either a minimal non-P_2-group, a minimal non-P-group which is a P_2-group, or a minimal irregular P-group.

For the property P_1, start with any minimal irregular group G of exponent p^2, and let H be the subgroup of $G \times C$ constructed in the proof of Theorem 25. Obviously $\operatorname{cl} H = \operatorname{cl} G$, and we claim that H is a minimal non-P_1-group. By [6, Proposition 11(g)], all proper subgroups of H are regular. Let Z be minimal normal in H. Then $Z \subseteq Z(H)$, and since H projects on G, we see that in $G \times C$, Z centralizes G, so

$$Z \subseteq \mho_1(G) \times C, \qquad Z \subseteq \mho_1(G) \times \mho_1(C) = \mho_1(G \times C) = \mho_1(H)$$

and therefore $|\mho_1(H/Z)| = p$ and H/Z is a P_1-group. This establishes our claim.

Notice that by choosing G above appropriately, we can have either $\Omega_1(H) = \Phi(H)$ or $\Omega_1(H)$ maximal in H. We do not know if $\Omega_1(H) = H$ is possible in a minimal non-P_1-group. In this example we also have $H' \neq \Phi(H)$. We do not know if $H' = \Phi(H)$ is possible. (Notice that if $H' \neq \Phi(H)$, then $K = H/H' \cap \mho_1(H)$, as a subdirect product of an abelian group and an exponent p group, is a P-group, and $|\mho_1(K)| = p$, so $\Omega_1(K) \neq K$, and also $\Omega_1(H) \neq H$). Nor do we know if minimal non-P_i-groups need to be as closely related to minimal irregular groups as in the examples constructed here.

References

1. J. R. J. Groves, On minimal irregular p-groups, *J. Austral. Math. Soc.* **16** (1973), 78–89.
2. P. Hall, A contribution to the theory of groups of prime power orders, *Proc. London Math. Soc.* **36** (1933), 29–95.
3. B. Huppert, "Endliche Gruppen I," Springer–Verlag, Berlin, 1967.
4. A. I. Kostrikin, The Burnside problem, *Izv. Akad. Nauk SSSR Ser. Mat.* **23** (1959), 3–34 [Russian; English translation, *Amer. Math. Soc. Transl.* **36** (1964), 63–99].
5. A. Mann, Regular p-groups, *Israel J. Math.* **10** (1971), 471–477.
6. A. Mann, Regular p-groups, II, *Israel J. Math.* **14** (1973), 294–303.
7. A. Mann, The power structure of p-groups II, to appear.
8. M. Suzuki, "Structure of a Group and the Structure of Its Lattice of Subgroups," Springer–Verlag, New York, 1956; cf. also F. Napolitani, Sui p-gruppi modulari finiti, *Rend. Sem. Mat. Padova* **39** (1967), 296–303.